NET MODULE
Maulbeerstrasse 10
CH-3011 Bern
Switzerland
info@netmodule.com
http://www.netmodule.com
Tel +41 31 985 25 10
Fax +41 31 985 25 11

Release Note NRSW 4.4.0.115

Project Name: NRSW

Abstract:

This document represents the release note for NetModule Router Software 4.4.0.115. It informs on new functionality, corrections and known issues of this software version of NetModule's router series.

Keywords:

NetModule, Software Development, NRSW, Release Note

Document Control:

Document:

Version	1.0
File	NRSW-RN-4.4.0.115
Status	Final

Creation:

Role	**Name**
Author	Moritz Rosenthal
Review	Benjamin Amsler

Approval

Role	**Name**
Director Product Development	Benjamin Amsler

1 Release Information

NetModule Router Software:

Version:	**4.4.0.115**
Date:	**Apr 21, 2022**

Supported Hardware:

NetModule Router	Hardware Version
NB800	V2.0 - V2.2, V3.2 (Rev. B02)
NB1600	V1.0 - V3.3
NB1601	V1.0 - V1.6
NB1800	V2.4 - V2.6
NB1810	V2.4 - V2.6
NB2700	V1.0 - V2.7
NB2710	V1.0 - V2.7
NB2800	V1.0 - V1.4
NB2810	V1.2
NB3700	V2.0 - V4.4
NB3701	V1.0 - V1.10
NB3710	V2.0 - V4.3
NB3711	V1.0 - V1.5
NB3720	V2.0 - V4.3
NB3800	V1.0 - V1.10

Unsupported Hardware:

NetModule Router
NB1300 Series
NB2200 Series
NB2300 Series
NB2500 Series
NB2600 Series

2 New Features

Case-#	Description
77573	**Random certificate key** On initial login from factory state a random key is generated to store generated and uploaded key encrypted internally. In the past a dedicated key had to be configured. This is still possible.

3 Security Fixes

The following security relevant issues have been fixed.

Case-#	Description
78103	**Linux kernel security patches** CVE-2022-0492 fixes a missing capabilities check for cgroups.
78106	**Security issues fixed in BusyBox package** CVE-2018-20679 and CVE-2019-5747: An out of bounds read in udhcp server, client and relay may allow a remote attacker to leak sensitive information from the stack by sending a crafted DHCP message. CVE-2018-1000500 and CVE-2021-42374 - CVE-2021-42386: These CVEs have been fixed in the source code even though they did not apply to the NRSW or were only exploitable by users with administrative status which have full access to the device anyway.
78655	**Security patches for mosquitto MQTT library** CVE-2017-7651: A possible DoS attack by memory exhaustion from unauthorized clients was fixed. CVE-2017-7654: A possible memory leak which could have been triggered by unauthorized clients was fixed. CVE-2017-7655: A possible NULL pointer dereference in the library was fixed. CVE-2018-12546: Clients still could subscribe to revoked topics and receive pending messages. This was fixed. CVE-2018-12550: A malformed ACL file could have circumvented the user authentication on the server side. CVE-2018-12551: A malformed configuration file could have circumvented the user authentication on the server side. CVE-2021-34432: The server will crash if the client sends a PUBLISH message with topic length of 0.
78803 **79179** **79180**	**OpenSSL security patches** CVE-2022-0778 fixed possible remote denial of service attack when parsing certificates. In NRSW only users with administrative rights may install certificates. Therefor the severity is considered low. CVE-2019-1547: A possible side channel attack in ECDSA signature operation was fixed. CVE-2019-1563: Possible Bleichenbacher padding oracle attack on RSA encryption keys fixed CVE-2020-1968: The Raccoon attack exploits a flaw in the TLS specification. The patch was back-ported. CVE-2021-23840: Possible integer overflow in the OpenSSL library fixed CVE-2021-23841: Possible NULL pointer deref in the OpenSSL library fixed CVE-2021-23839: Version rollback attack when unpadding an RSA signature fixed.
78954	**CVE-2018-25032 zlib denail of service** The compression library zlib was vulnerable to a memory corruption when compressing input with distant matches. The upstream patches were back-ported to NRSW.

4 Fixes

The following issues and problems have been fixed.

Case-#	Description
74590 **75946** **77596** **78157** **78477**	**GUI improvements** The initial password setup did not deny non-ASCII characters in the user password. Never the less these characters were not handled correctly resulting in a device where the user could not log in. This was fixed. Now non-ASCII characters are rejected with an appropriate error message. A failure was fixed that prevented to set up ToS based extended routing filters. An Ethernet WAN link was not removed from the WAN link list if the corresponding Ethernet interface was bridged to another logical LAN interface. This was fixed. The system status page did not show the correct system power supply voltage range. The value was changed to meet the requirements from the manual and the specification plate. It was not possible to set client routes while the OpenVPN server was enabled. This was fixed.
74832	**WLAN AP configuration with automatic channel selection could fail** In some situations the WLAN Access-Point with automatic channel selection did not start up correctly due to a timing issue. This was fixed.
74962	**Bridged VLAN blocks broadcast packets** The hardware switch chip drops VLAN tagged broadcast packets if a VLAN is bridged with an Ethernet interface. This was fixed by disabling the HW offload in such situations.
75219	**Single WWAN network configuration failed on Toby-L2** It could happen that 2G- 3G- or 4G-only configurations did not connect to the network even though the network was available. This was fixed.
75844	**2nd DNS relay service does not work** Configurations with different DNS relay servers for different interfaces did not work. This was fixed.
77469	**Shell code injection via PHP-CLI** Users with administrative right could inject shell code via PHP-CLI if PHP-CLI was enabled. PHP-CLI gives the authenticated administrative user full access to the device configuration. Therefore this is considered undesired behavior which was fixed and not a security issue.

5 Known Issues

Items listed here represent minor problems known at release time. These issues will be resolved in a later version.

Case-#	Description
78673	**MQTT Broker** The broker does not reject strings that are not valid UTF-8. As a result, a malicious client could cause other clients, that do reject invalid UTF-8 strings, to disconnect themselves from the broker by sending a topic string which is not valid UTF-8, and so cause a denial of service for the clients. If this is a problem for your application we recommend to NRSW 4.6 or newer which uses a more recent version of the MQTT mosquitto library which does not have this issue. A safe back-port of the patches fixing this bug was not possible.

6 ECC conversion

The flash on NB1600, NB2700, NB2710, NB3700, NB3710 and NB3720 provides an automated error correction using ECC. With release 4.1.0.100 we changed the ECC length from 1-bit ECC to 4-bit ECC which provides better error correction. On first boot after the update was performed the data on the flash is automatically converted to use the new ECC setup. While this conversion is performed the LEDs show a running light for about 30 seconds.
If you switch back to an older software release like 4.0.0 the migration is reverted.
We tested updates and down-grades to and from 4.0.0 and 3.8.0. Updates to or from older versions are not supported. If you run an older release or want to downgrade to an older release or a feature release like 3.8.2 you are advised to migrate via 4.0.0 as an intermediate release.
To revert the migration on downgrade the SPL boot loader release 4.1.0 stays in place. It can be downgraded in a second sofware update process initiated from the target release after the first reboot.
Software updates with recovery images require special attention. You must not use recovery images 4.0.0 and older for systems running 4.1.0 and newer.
If you want to use recovery images please contact our support at router@support.netmodule.com.

7 OSS Notice

We inform you that NetModule products may contain in part open source software. We are distributing such open source software to you under the terms of GNU General Public License (GPL)[1], GNU Lesser General Public License (LGPL)[2] or other open source licenses[3].
These licenses allow you to run, copy, distribute, study, change and improve any software covered by GPL, Lesser GPL, or other open source licenses without any restrictions from us or our end user license agreement on what you may do with that software. Unless required by applicable law or agreed to in writing, software distributed under open source licenses is distributed on an "AS IS" basis, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
To obtain the corresponding open source codes covered by these licenses, please contact our technical support at router@support.netmodule.com.

[1] GPLv2 license is available at http://www.gnu.org/licenses/gpl-2.0.txt
[2] LGPL license is available at http://www.gnu.org/licenses/lgpl.txt
[3] OSI licenses (ISC License, MIT License, PHP License v3.0, zlib License) are available at http://opensource.org/licenses

8 Change History

Version	Date	Name	Reason
1.0	Apr 21, 2022	Moritz Rosenthal	Final release note

NetModule AG is located at:

Maulbeerstrasse 10
CH-3011 Bern
Switzerland

info@netmodule.com
Tel +41 31 985 25 10
Fax +41 31 985 25 11

For more information about NetModule AG visit the NetModule website at *www.netmodule.com.*